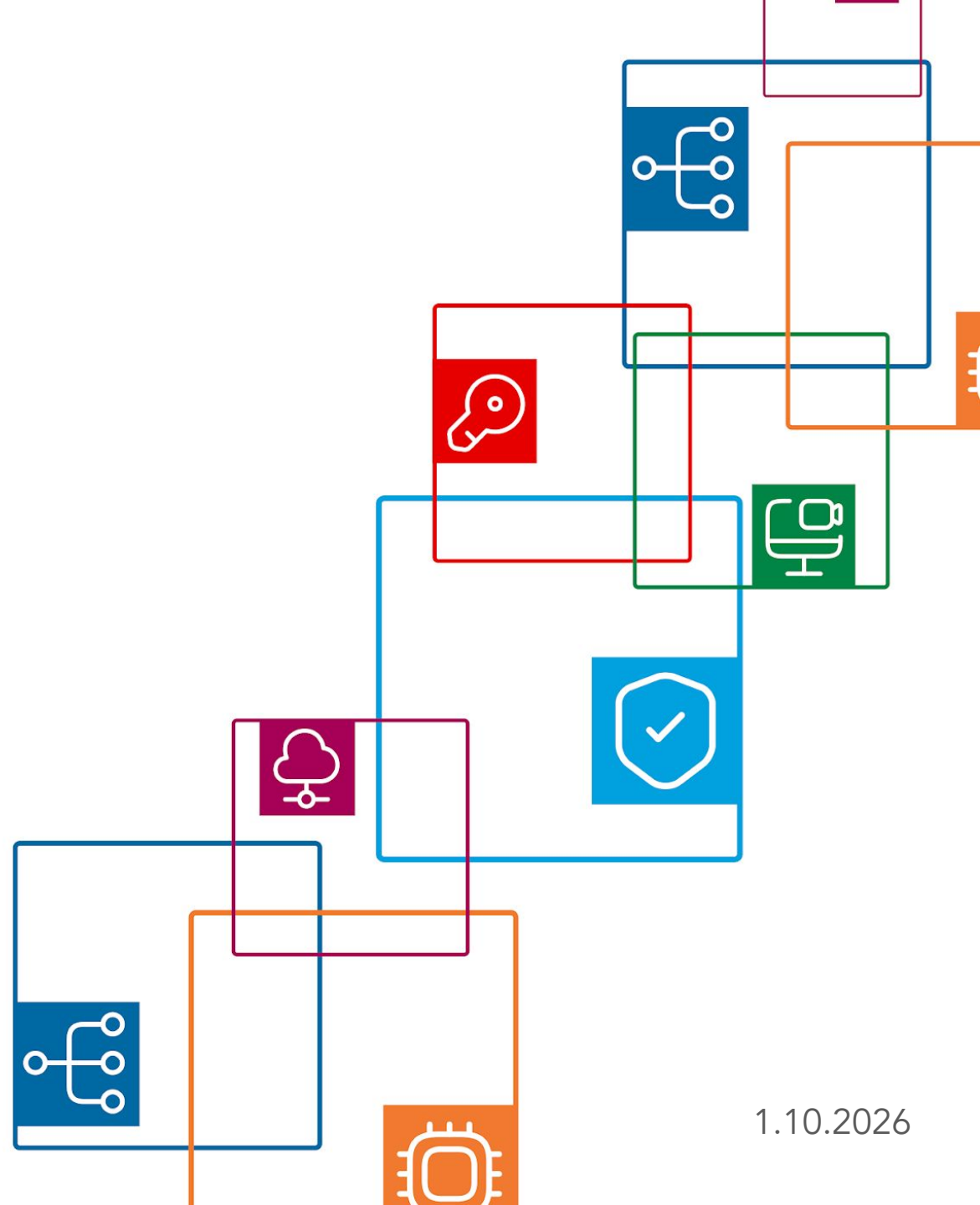


Digitální peněženka

Martin Kuba <makub@cesnet.cz>

konference e-infrastruktury CESNET 2026

track Bezpečnost





- členské státy EU mají do konce roku 2026 povinnost poskytnout svým občanům tzv. EUDIW - EU Digital Identity Wallet
- DIA to překládá jako „Evropská peněženka digitální identity“
- není to peněženka, je to dokladovka, bude obsahovat doklady
 - kvalifikované
 - občanský průkaz
 - řidičský průkaz, technický průkaz auta
 - ISIC, univerzitní diplom
 - průkaz zdravotního pojištění
 - nekvalifikované
 - členská karta do fitness klubu
 - průkaz zaměstnance
 - vlaková jízdenka, letenka
- **nebudou v ní peníze**
 - žádné kryptoměny, kredity, ani nic podobného
 - s pomocí dokladu asi půjde podat platební příkaz v bankovní aplikaci





- eIDAS 1.0 eID (tzv. „Identita Občana“)

- inter-federace národních autentizačních schémat
- protokol SAML (Security Assertion Markup Language)
- web server IdP (Identity Provider) vydává XML dokument web serveru SP (Service Provider)
- **problém č. 1** - IdP ví o každém přihlášení uživatele
- **problém č. 2** - eID je v mnoha zemích včetně ČR uměle omezeno na orgány veřejné moci

- eIDAS 2.0 EUDIW

- aplikace (mobilní nebo webová)
- protokoly OID4VC (OpenID for Verifiable Credentials)
- sbírá doklady od vydavatelů (Issuer)
- vydává doklady příjemcům (Verifier)
- problém č.1 vyřešen - vydavatel neví, kde a kdy jsou doklady použity
- problém č.2 by měl být vyřešen - tzv. nekvalifikovaní vydavatelé



Components of the “OpenID for Verifiable Credentials” specification family



③ **OpenID for Credential Issuance** (Issuance of verifiable credentials)

① **OpenID Connect for Verifiable Presentations** (Presentation of verifiable credentials)

② **Self-Issued OP v2** (authentication using identifiers not namespaced to the third-party identity providers)



- možná budeme moci přijímat doklady vydané státem
 - hodí se to při zpracování citlivých dat
- možná budeme moci přijímat doklady vydané jinými státy EU
 - zatím neexistuje použitelná možnost on-line ověření s LoA substantial
- možná budeme moci vydávat vlastní doklady
 - virtuální průkazku uživatele e-infrastruktury
 - virtuální průkazku akademického výzkumníka
- možná budeme moci v našich dokladech použít JSON-Linked Data
 - bohatší strukturované informace o uživateli díky RDF
 - např. „výzkumník z nekomerční organizace zkoumající rakovinu“



- primární doklad bude tzv. PID - Personal Identification Data
 - family_name, given_name, birth_date, birth_place, nationality, portrait
 - záměrně neobsahuje identifikátor uživatele, aby nešlo uživatele sledovat napříč službami
 - to komplikuje identifikaci
 - při změně osobních údajů se změní PID
 - patrně bude nutné vytvářet ad hoc identifikátory, např. identifikátor uživatele e-infrastruktury
- česká EUDIW bude dostávat PID jen pro lidi v ROB (registr obyvatel)
 - obsahuje:
 - občany ČR
 - cizince s trvalým pobytem
 - cizince s přechodným pobytem delším než 90 dnů
 - cizince s uděleným azylem
 - zahraniční studenty
 - přeshraniční pracovníky



- **PuB-EAA - Public Electronic Attestations of Attributes**
 - LoA high - data od úředních orgánů z registrů státu
 - ekvivalent papírových dokumentů - rodný list, řidičský průkaz, ...
 - vydávají státní orgány uvedené v EU Trust List
- **QEAA - Qualified Electronic Attestations of Attributes**
 - LoA high - od důvěryhodných prostředníků napojených na státem akreditované subjekty (vysoké školy, profesní komory, zdravotní pojišťovny, ...)
 - VŠ diplomy, profesní kvalifikace (advokátní oprávnění, lékařské licence), pilotní průkazy, výpisy z obchodního rejstříku, ...
 - vydávají Qualified Trust Service Providers (QTSPs) uvedení v EU Trust List
- **EAA - Non-Qualified Electronic Attestations of Attributes**
 - LoA low nebo substantial - ostatní vydavatelé dokladů
 - členské průkazky, zaměstnanecké průkazky, jízdenky, věrnostní karty, ...
 - vydávají non-qualified Trust Service Providers (TSPs), scheme-specific trust list



- OID4VC rozlišuje mezi Verifiable Credentials (VC) a Verifiable Presentations (VP)
 - doklad prezentovaný příjemci se může skládat z více vydaných dokladů a zároveň některé údaje vynechat
- např. můžete předložit svoje jméno bez bydliště nebo roku narození
- speciální je ověření věku - VC obsahuje sadu příznaků

age_over_15	Starší než 15 let	BOOLEAN
age_over_18	Starší než 18 let	BOOLEAN
age_over_21	Starší než 21 let	BOOLEAN
age_over_60	Starší než 60 let	BOOLEAN
age_over_65	Starší než 65 let	BOOLEAN

- IETF SD-JWT VC pro on-line ověřování přes internet
 - IETF - Internet Engineering Task Force
 - SD-JWT - Selective Disclosure for JSON Web Tokens
 - RFC 9901, rozšíření formátu JWT (RFC 7519) o volitelná „odhalení“ dat
- ISO/IEC-mdoc pro blízké ověřování přes BLE, NFC, QR kódy
 - ISO - International Organization for Standardization
 - IEC - International Electrotechnical Commission
 - mdoc - mobile document format
 - založen na formátu CBOR - Concise Binary Object Representation - RFC 8949
- W3C Verifiable Credentials Data Model 2.0
 - v EUDIW odloženo, není v seznamu podporovaných formátů
 - založen na JSON-Linked Data reprezentaci RDF (semantic web)



- JWT je text tvaru **<header>.<payload>.<signature>**
 - header obsahuje údaje o podepisujícím klíči a algoritmu
 - payload je JSON
 - všechny tři části jsou zakódované base64url
- SD-JWT je text tvaru **<header>.<payload>.<signature>~<d1>...~<dN>~<keybinding>**
 - payload obsahuje hashe jednotlivých disclosures
 - disclosure je JSON trojice [**<salt>**, **<claim name>**, **<claim value>**]
 - při prezentaci jsou přidány jen disclosure toho, co je nutné poskytnout
 - keybinding je veřejný klíč Holdera (walletu)
 - tj. SD-JWT je něco jako X509 certifikát, kde CA je Issuer, subject je Holder



Encoded SD-JWT

eyJ0eXAiOiJzZCtqd3QiLCJhbGciOiJFUzI1NiJ9.eyJpZCI6IjEyMzQlLCJf
c2QiOiSiYkRUUnZtNS1Zbi1IRzdjcXBWUjVPVlJJWHNTYUJrNTdKZ2IPc
V9qMVZJNCIsmV0M1VmUnisd1ZyZlhkUeT6Zzc5aGNqRDFJdHpvUTI
vQm9YUkd0TW9zRmsiLCJ6V2ZaTIMxOUF0YIJTVGJvN3NKUm4wQl
pRdlIdSZGNob0M3VVphYkZyalk4lI0slI9zZF9hbGciOiJzaGEtMjU2Ln0.n
27NCtnuwytIBYtUNjgkesDP_7gN7bhaLhWNL4SWT6MaHsOjZ2ZMp9
87GgQRL6ZkLbJ7Cd3hlePHS84GBXPuv~WyI1ZWl4Yzg2MjM0MDJj
ZjJlliwiZmlyc3RuYW1lliwiSm9obiJd~WyJjNWZmZWY2ZWYzNTg4MW
JjliwibGFzdG5hbWUiLCJeb2UiXQ~WyJmYTlkYTUzZWJjOTk3OTlliwi
c3NuliwiMTIzLTQ1LTQ1ODkiXQ~eyJ0eXAiOiJrYitqd3QiLCJhbGciOiJF
UzI1NiJ9.eyJpYXQiOiE3MTAwNjk3MjIsmF1ZCI6ImRpZDpleGFtcGxIOj
EyMyIsIm5vbmNlIjoiazh2ZGYwbmQ2liwic2RfaGFzaCI6ImRtTmJWSzN
mczI3VzNHhDNouktsNEt1NmZDMUwzN0R2MFFfaIBXkd0ppRkUifQ.p
qw2OB5IA5ya9Mxf60hE3nr2gsJEIollnuCa4qlisijHbwg3WzTDFmW2S
uNvK_ORN0WU6RoGbJx5uYZh8k4EbA

<https://www.sdjwt.co/>

Header		
1	{	
2	"alg": "ES256",	
3	"typ": "sd+jwt"	
4	}	
Payload		Disclosure
1	{	
2	"id": "1234",	Salt: 5eb8c8623402cf2e
3	"_sd": [	Key: firstname
4	"bDTRvm5-Yn-	Value: John
5	HG7cqpVR5OVRIXsSaBk57JgiOq_j1VI4",	Salt: c5c31f6ef35881bc
6	"et3UfRylwVrfXdPKzg79hcjD1ltzoQ9oBoXR	Key: lastname
7	GtMosFk",	Value: Doe
8	"zWfZNS19AtbRSTbo7sJRn0BZQvWRdcho	
9	C7UZabFrjY8"	
10	],	Salt: fa9da53ebc99798e
11	"_sd_alg": "sha-256"	Key: ssn
12	}	Value: 123-45-6789

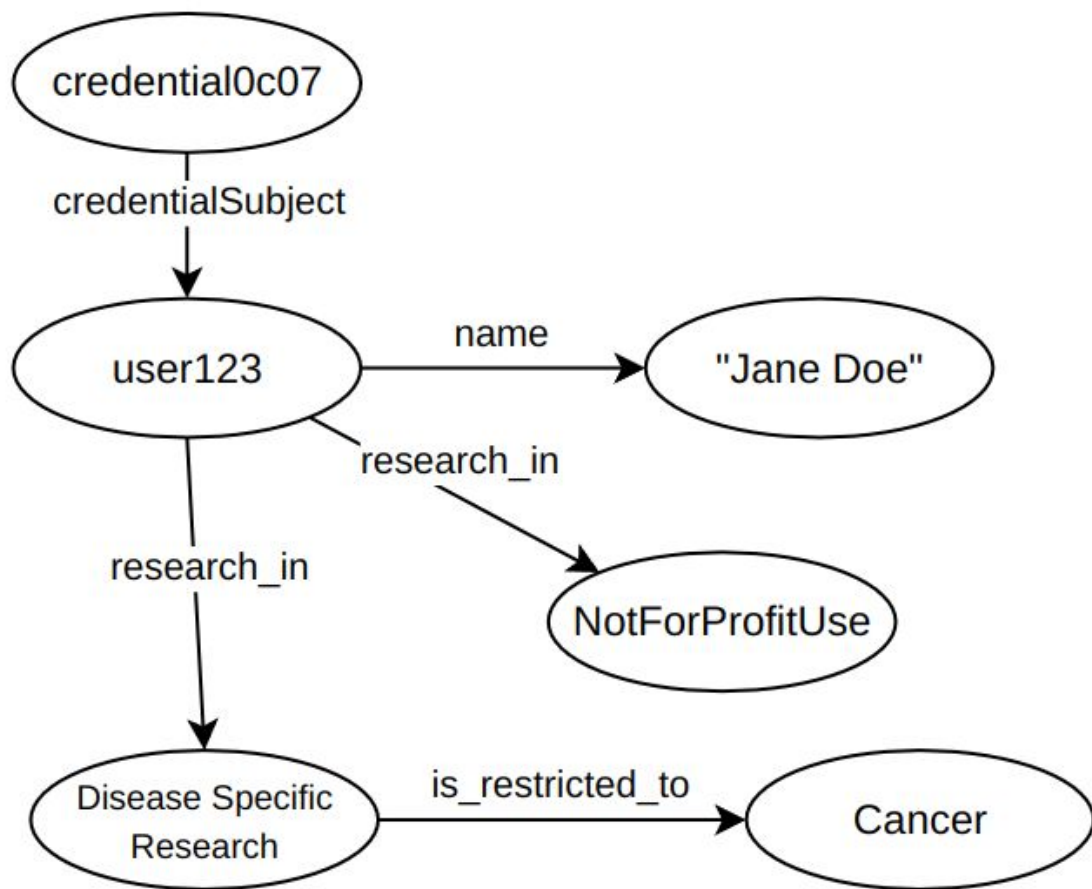
Key Binding Header		Key Binding Payload	
1	{	1	{
2	"typ": "kb+jwt",	2	"iat": 1710069722,
3	"alg": "ES256"	3	"aud": "did:example:123",
4	}	4	"nonce": "k8vdf0nd6",
		5	"sd_hash": "_-
		6	NbVK3fs9wW3Gh3NRKR4Ku6fC1L37Dv0Q_
			jPWwJiFE"
			}

- RFC draft <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>
 - JWT header type „dc+sd-jwt” (dc - digital credential)
- definuje nové claims pro SD-JWT
 - vct (verifiable credential type) - URL na metadata pro daný typ VC
 - aka_vcts - další typy, kterým také odpovídá
- metadata pro typ VC obsahují:
 - claim metadata - co claimy znamenají a zda jsou povinné
 - display metadata - jak se claimy jmenují v různých jazycích/locales
 - rendering metadata - jak zobrazit claimy pomocí SVG šablon
 - zda je typ rozšíření (extension) jiného typu



- RFC 8949 Concise Binary Object Representation (CBOR)
- v podstatě binární JSON
- podobné ASN.1 použitému v LDAP a X509 certifikátech
- viděli jste v „EU Digital COVID Certificate“ v jeho QR kódu





```
"@context": [  
  "https://www.w3.org/ns/credentials/v2",  
  "https://ga4gh.org/ns/contexts/visas.jsonld"  
],  
"id": "urn:uuid:0c07c1ce-57cb-41af-bef2-1b932b986873",  
"type": ["VerifiableCredential", "Ga4ghPassportVisa"],  
"issuer": "https://login.aai.lifescience-ri.eu/",  
"validFrom": "2025-04-01T05:28:04Z",  
"credentialSubject": {  
  "id": "https://login.aai.lifescience-ri.eu/users/123",  
  "name": "Jane Doe",  
  "research_in": [  
    "NotForProfitUse",  
    { "type": "DiseaseSpecificResearch", "is_restricted_to": "Cancer" }  
  ]  
}
```



normální JSON

```
{
  "name": "John Doe",
  "children": [ "Alice" ],
  "address": {
    "street": "1201 N Muldoon Rd",
    "city": "Anchorage"
  }
}
```

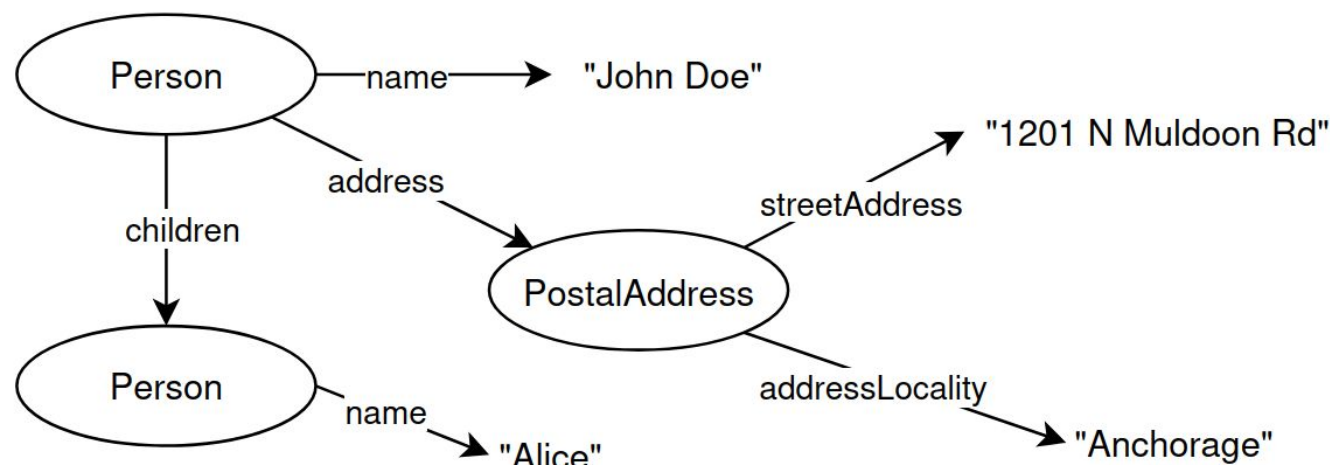
JSON-LD s typováním a odkazy do slovníků

```
{
  "@type": "https://schema.org/Person",
  "https://schema.org/name": "John Doe",
  "https://schema.org/children": [
    { "@type": "https://schema.org/Person",
      "https://schema.org/name": "Alice" }
  ],
  "https://schema.org/address": {
    "@type": "https://schema.org/PostalAddress",
    "https://schema.org/streetAddress": "1201 N Muldoon Rd",
    "https://schema.org/addressLocality": "Anchorage"
  }
}
```

odkaz do slovníku
na definici typu / třídy

odkaz do slovníku na definici
relace / predikátu

RDF graf



úsporný JSON-LD s kontextem

```
{
  "@context": {
    "@vocab": "https://schema.org/"
  },
  "@type": "Person",
  "name": "John Doe",
  "children": [ { "@type": "Person", "name": "Alice" } ],
  "address": {
    "@type": "PostalAddress",
    "streetAddress": "1201 N Muldoon Rd",
    "addressLocality": "Anchorage"
  }
}
```

prefix slovníku

pojmy ze slovníku

- ontologie je strukturovaný slovník, dokument se soupisem pojmů a jejich vztahů
 - třídy
 - relace mezi třídami (hierarchie, taxonomie)
 - individua ve třídách
- existuje W3C specifikace jazyka OWL (Web Ontology Language)
- ujal se zejména v lékařství a biologii
 - Mondo Disease Ontology
 - Data Use Ontology



Class hierarchy: cancer

Asserted

- cancer or benign tumor
 - cancer-related condition
 - hyperplasia
 - neoplastic disease or syndrome
 - neoplasm
 - abducens nerve neoplasm
 - ACTH-producing pituitary gland neoplasm
 - adrenal cortex neoplasm
 - adrenal gland neoplasm
 - adrenal medulla neoplasm
 - ampulla of vater neoplasm
 - anal gland neoplasm
 - anus neoplasm
 - apocrine sweat gland neoplasm
 - appendiceal neoplasm
 - autonomic nervous system neoplasm
 - axillary neoplasm
 - Bartholin gland neoplasm
 - basal cell neoplasm
 - benign neoplasm
 - bile duct neoplasm
 - biliary tract neoplasm
 - blood vessel neoplasm
 - bone marrow neoplasm
 - bone neoplasm
 - brachial plexus neoplasm
 - brain neoplasm
 - brainstem neoplasm
 - breast neoplasm
 - bronchial adenomas/carcinoids
 - bronchial neoplasm
 - buccal mucosa neoplasm
 - cancer**
 - ACTH-producing pituitary gland neoplasm

Class Annotations

Class Usage

Annotations: cancer

Annotations +

rdfs:label

cancer

id

[MONDO:0004992](#)

definition

A tumor composed of atypical neoplastic, often pleomorphic cells that invade other tissues. Malignant neoplasms often metastasize to distant anatomic sites and may recur after excision. The most common malignant neoplasms are carcinomas (adenocarcinomas or squamous cell carcinomas), Hodgkin and non-Hodgkin lymphomas, leukemias, melanomas, and sarcomas.

Description: cancer

neoplasm

General class axioms +

SubClass Of (Anonymous Ancestor)

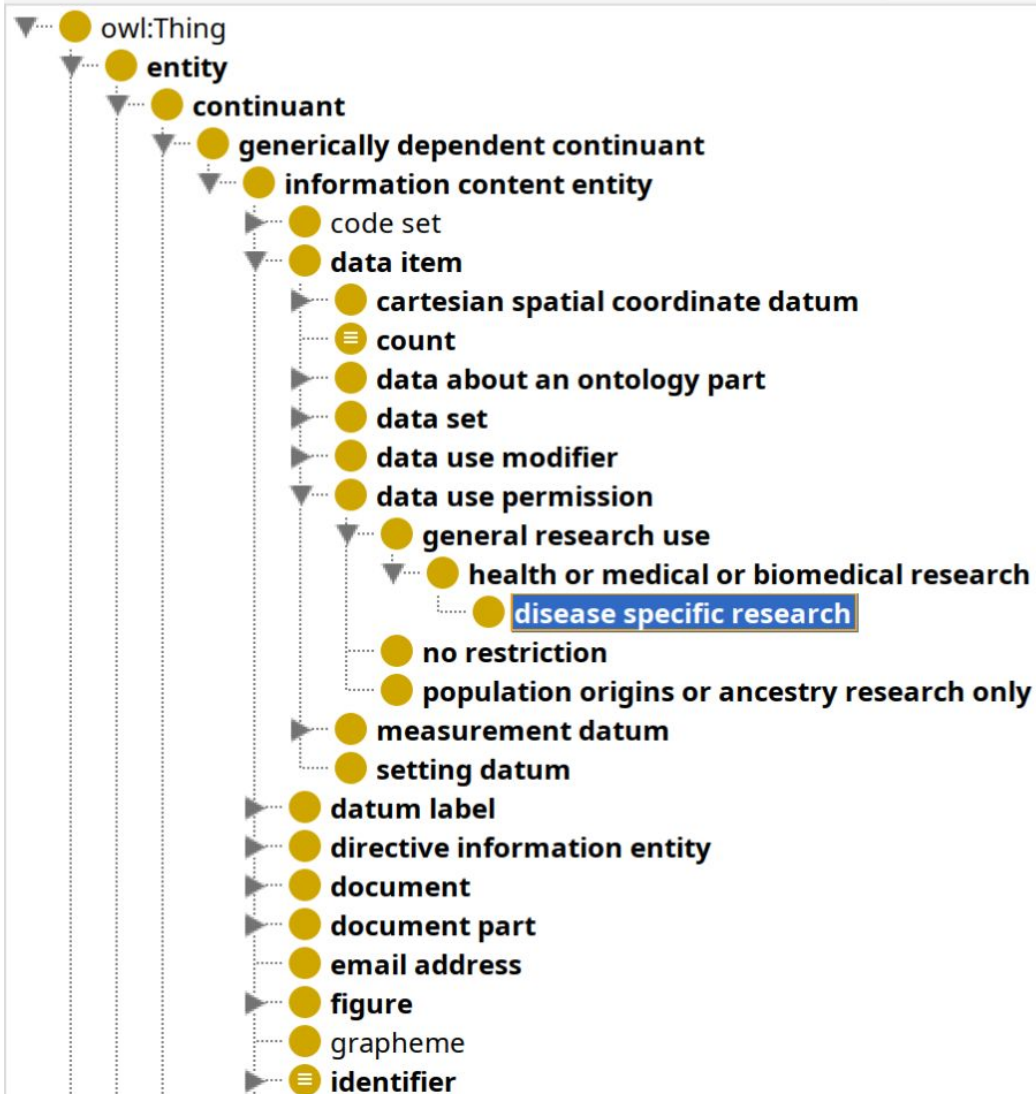
- 'disease causes disruption of' some 'cell population proliferation'
- hyperplasia or 'precancerous condition' or 'neoplastic disease or syndrome' or 'cancer-related condition'
- 'human disease' and ('disease causes disruption of' some 'cell population proliferation')
- neoplasm or 'neoplastic syndrome'
- 'in taxon' some 'Homo sapiens'
- disease and ('in taxon' some 'Homo sapiens')

Instances +

Class hierarchy: disease specific research



Asserted ▼



Annotations: disease specific research



Annotations +

rdfs:label [language: en]

disease specific research

**id**[DUO:0000007](#)**definition** [language: en]

This data use permission indicates that use is allowed provided it is related to the specified disease.

**rdfs:comment** [language: en]

This term should be coupled with a term describing a disease from an ontology to specify the disease the restriction applies to.



DUO recommends MONDO be used, to provide the basis for automated evaluation. For more information see https://github.com/EBISpot/DUO/blob/master/MONDO_Overview.md

Other resources, such as the Disease Ontology, HPO, SNOMED-CT or others, can also be used. When those other resources are being used, this may require an extra mapping step to leverage automated matching algorithms.

Description: disease specific research



Equivalent To +

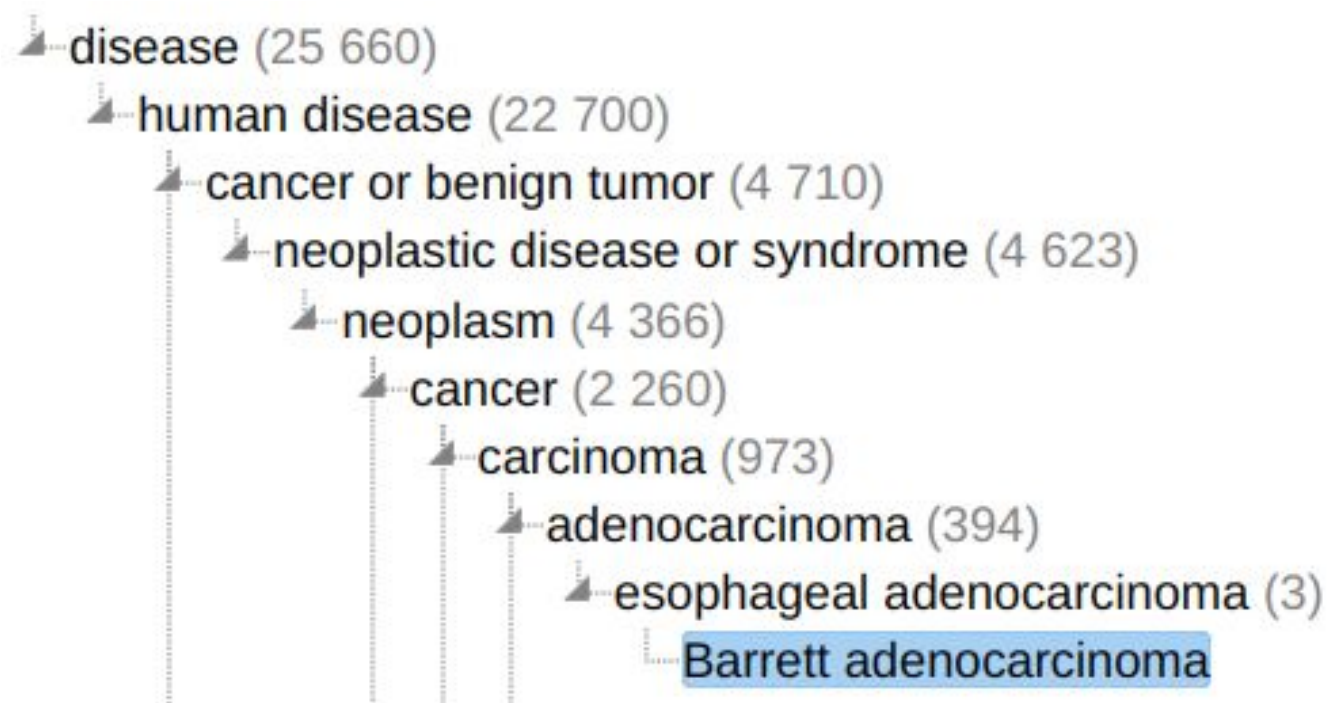
SubClass Of +

'health or medical or biomedical research'

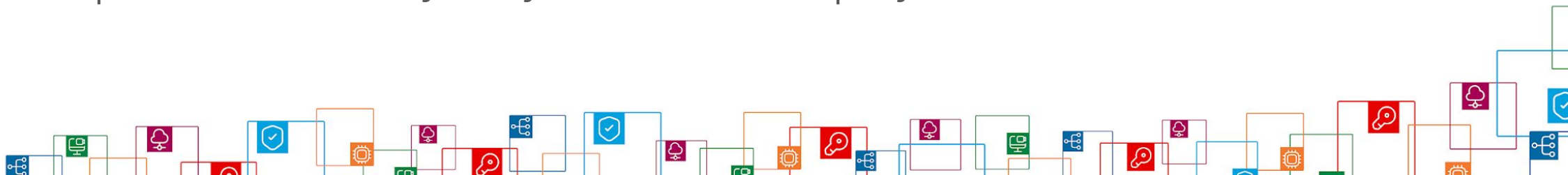
'is restricted to' some 'disease or disorder'



hierarchie tříd umožňuje odvozovat, např. že výzkum nemoci „Barrett adenocarcinoma“ je zároveň výzkumem rakoviny a výzkumem lidské nemoci



- pokud by
 - uživatel měl VC s údajem, že provádí výzkum „Barrett adenocarcinoma“
 - dataset měl údaj, že přístup mají jen výzkumníci v oboru rakoviny
- dá se automaticky rozhodnout, že tento uživatel splňuje podmínky přístupu k datasetu (OWL reasoner)
- současný stav
 - výzkumník podá žádost o přístup k datasetu
 - sejde se lidská komise, schválí žádost a přidá ho do skupiny s povolením přístupu k datasetu
 - autorizace ověřuje jen členství ve skupině
 - problém může být s vyřazením ze skupiny



- OpenID for Verifiable Credential Issuance 1.0 (2025-09-16)
 - https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html
- OpenID for Verifiable Presentations 1.0 (2025-07-09)
 - https://openid.net/specs/openid-4-verifiable-presentations-1_0.html
- OpenID4VC High Assurance Interoperability Profile 1.0 (2025-12-24)
 - https://openid.net/specs/openid4vc-high-assurance-interoperability-profile-1_0-final.html
- Self-Issued OpenID Provider v2 (draft 13)
 - https://openid.net/specs/openid-connect-self-issued-v2-1_0.html
- Presentation Exchange 2.1.1(2024-07-30)
 - <https://identity.foundation/presentation-exchange/spec/v2.1.1/>
- SD-JWT-based Verifiable Digital Credentials (draft 19)
 - <https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/>



- OID4VC peněženky - nové paradigma self-sovereign identity
- EUDIW
 - primární PID
 - public, qualified a non-qualified EEAs
- selektivní vydávání atributů
- formáty dokladů
 - VC-SD-JWT
 - mdoc (CBOR)
 - VCDM 2.0 s JSON-LD/RDF

